Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 89 (2013)

On testing bent functions

Abhishek Bhrushundi

Chennai Mathematical Institute
India
abhishek_bhr@cmi.ac.in

Abstract. A bent function is a Boolean function all of whose Fourier coefficients are equal in absolute value. These functions have been extensively studied in cryptography and play an important role in cryptanalysis and design of cryptographic systems.
We study bent functions in the framework of property testing. In particular, we show that testing whether a given Boolean function on n variables is bent, or $\frac{1}{8}$-far from being bent, requires $\Omega(n^2)$ queries.
As an intermediate step in our proof, we show that the query complexity of testing if a given function is a quadratic bent function, or $\frac{1}{4}$-far from being so, is $\Theta(n^2)$. We remark that this problem is equivalent to testing affine-isomorphism to the inner product function.
Our proof exploits the recent connection between property testing and parity decision trees due to Chakraborty and Kulkarni. We believe our techniques might be useful in proving lower bounds for other properties of quadratic polynomials.

1 Introduction

1.1 Bent functions

Bent functions are Boolean functions for which all the Fourier coefficients are equal in absolute value. These functions were first defined and studied by Rothaus [14]. Bent functions tend to maximize what is known as the *nonlinearity* of a Boolean function, defined as the hamming distance of the function from the set of all affine functions, which is an important measure of cryptographic quality and is often used in cryptanalysis. Due to this, and other nice properties, bent functions find a variety of applications in cryptography, coding theory, and combinatorial design. The interested reader may refer to [11] for more information.

1.2 Property testing

Property testing deals with *testing* some property of an object by a tester with unbounded computational power and given oracle access to the object. The job of the tester is to determine (with high probability) whether the object satisfies the property or is *far* from satisfying the property. The complexity of the tester is measured in terms of the number of queries it makes to the oracle in the worst-case scenario.

ISSN 1433-8092

A property $\mathcal{P}$ of Boolean functions is a collection of Boolean functions. A two-sided tester T for $\mathcal{P}$ is a randomized algorithm which, given oracle access to input $f : \mathbb{F}_2^n \to \mathbb{F}_2$, and an input parameter ϵ:

- accepts f with probability greater than $\frac{2}{3}$, if $f \in \mathcal{P}$.
- rejects f with probability greater than $\frac{2}{3}$, if it is ϵ-far from $\mathcal{P}$.

By ϵ-far we mean that f differs from every function in $\mathcal{P}$ in at least ϵ-fraction of points in $\mathbb{F}_2^n$.
The query complexity of T is the worst-case number of points at which it queries the value of the input function. The query complexity of testing $\mathcal{P}$ is the query complexity of the best tester that tests $\mathcal{P}$, and may depend on both n and ϵ.
See [2,7,15] for an overview of testing properties of Boolean functions and property testing in general.

1.3 Testing bent functions

In this paper, we are primarily interested in the problem of testing bent functions. In an intermediate step, we study the problem of testing whether a given function is a quadratic bent function (by quadratic, we shall always mean polynomials of degree at most two) or far from being so.

Motivation With respect to nonlinearity, testing bent functions is in some sense the "opposite" of linearity testing, since linear functions have the lowest possible value of nonlinearity. Linearity can be tested in constant number of queries [3], and an interesting problem then is to determine the query complexity of testing the other extreme i.e. bent functions.

The intermediate problem we study is equivalent to testing if a given function is isomorphic to the inner product function under the action of invertible affine transformations. We remark that problems of this nature i.e. testing isomorphism under the action of a group, have been studied before: [8] gives conditions under which affine and linear isomorphism to a given function are testable in constant number of queries, [4] does the same for testing isomorphism under the action of S_n.

Our Results Our first result concerns testing quadratic bent functions:

Theorem 1. *Any adaptive two-sided tester for $\frac{1}{4}$-testing the set of quadratic bent functions must make $\Omega(n^2)$ queries.*

Here, by ϵ-testing, we mean testing to determine if the input is in the property or is ϵ-far from it. We remark that Theorem 1 is tight since a folklore result gives a tester with quadratic query complexity.
We then prove our main result:

Theorem 2. *Any adaptive two-sided tester that $\frac{1}{8}$-tests the set of bent functions must make $\Omega(n^2)$ queries.*

Note that we do not have a matching upper bound for the general problem. In fact, to the best of our knowledge, no nontrivial upper bound is known.

1.4 Proof techniques

Recently [5] gave a technique to characterize the query complexity of testing properties of linear functions in terms of parity decision tree complexity. Specifically, they show that the query complexity of testing a linear function property $\mathcal{P}$ can be lower bounded by the randomized decision tree complexity of a related function $E_{\mathcal{P}}$.

The proof of Theorem 1 exploits the observation that the above characterization works even when one looks at certain properties of quadratic functions, in particular, the property of being bent. For the property of quadratic bent functions, $E_{\mathcal{P}}$ turns out to be a function mapping the set of undirected simple graphs on n vertices to $\mathbb{F}_2$, such that $E_{\mathcal{P}}(G) = 1$ iff the adjacency matrix of G is nonsingular.
The proof then proceeds to lower bound the randomized decision tree complexity of $E_{\mathcal{P}}$. This is done by analyzing the communication complexty of an XOR function related to $E_{\mathcal{P}}$, an idea used in [5].

A result due to Chen et al.[6] shows that, if two properties $\mathcal{P}_1$ and $\mathcal{P}_2$ satisfy a certain condition, their intersection $\mathcal{P}_1 \cap \mathcal{P}_2$ is testable with query complexity being roughly the sum of the query complexities of $\mathcal{P}_1$ and $\mathcal{P}_2$.
Say $\mathcal{P}_1$ is the set of bent functions, and $\mathcal{P}_2$ the set of quadratic functions. We know that $\mathcal{P}_2$ is testable in constant number of queries[1]. Thus, if we can show that $\mathcal{P}_1$ and $\mathcal{P}_2$ satisfy the above condition, lower bounding the query complexity of $\mathcal{P}_1 \cap \mathcal{P}_2$ would prove a lower bound on the query complexity of $\mathcal{P}_1$. Since 1 already gives us a quadratic lower bound on the query complexity of $\mathcal{P}_1 \cap \mathcal{P}_2$, all that is left in order to prove Theorem 2 is to show that $\mathcal{P}_1$ and $\mathcal{P}_2$ satisfy the required condition.

This condition essentially says that the set of bent functions that are not quadratic is "far" from the set of quadratic functions that are not bent. We prove that this condition is indeed satisfied by using the powerful structure theorem for quadratic polynomials over $\mathbb{F}_2$[10].

1.5 Organization

We begin by introducing a few important definitions in Section 2. In Section 3, we prove a lower bound of $\Omega(n^2)$ on testing quadratic bent functions, after which we proceed to proving a lower bound for testing general bent functions in Section 4. Finally, in Section 5, we describe a folklore result which gives a tight upper bound for testing quadratic bent functions.

2 Preliminaries

2.1 Boolean functions and their Fourier transform

We introduce the basics of Boolean function analysis. The treatment here is far from complete, and the reader may refer to [13] for a detailed account.
We shall regard a Boolean function f as a function mapping $\mathbb{F}_2^n$ to $\mathbb{F}_2$. For reasons

that shall become clear later, we shall only look at the case when n is even.
For two boolean functions f and g, by $dist(f,g)$ we shall mean the fraction of points of $\mathbb{F}_2^n$ at which $f(x) \neq g(x)$.
Recall that f can also be viewed as a function mapping $\mathbb{F}_2^n$ to $\mathbb{R}$ by looking at $(-1)^{f(x)}$. For a subset $S \subseteq [n]$, $\chi_S(x) := (-1)^{\sum_{i \in S} x_i}$ i.e. the parity on the variables contained in S. These are called *character* functions.
Consider the space of all functions from $\mathbb{F}_2^n$ to $\mathbb{R}$, equipped with the inner product $\langle f, g \rangle = \mathbb{E}_x f(x)g(x)$. It is not hard to verify that the character functions form an orthonormal basis with respect to the above inner product. Thus, for any function $f : \mathbb{F}_2^n \to \mathbb{R}$,

$$f(x) = \sum_{S \subseteq [n]} \hat{f}(S)\chi_S(x)$$

$(\hat{f}(S))_{S \subseteq [n]}$ is called the *Fourier transform* of f, where the *Fourier coefficient* $\hat{f}(S)$ can be computed as follows:

$$\hat{f}(S) = \langle f, \chi_S \rangle$$

It is also useful to define the following norm of the Fourier transform:

Definition 1. *The Fourier norm of a function f is defined as the l_1 norm of its Fourier transform i.e $\sum_{S \subseteq n} |\hat{f}(S)|$. We shall denote it by $\|\hat{f}\|_1$.*

The following lemma will play an important role in our proofs:

Lemma 1. *Let $f : \mathbb{F}_2^n \to \mathbb{R}$, $A \in GL_n(\mathbb{F}_2)$, and $U \subseteq [n]$. Let $h(x) = (f \circ A)(x) \times \chi_U(x)$, then $\{|\hat{f}(S)|\}_{S \subseteq [n]}$ and $\{|\hat{h}(T)|\}_{T \subseteq [n]}$ are equal as multisets. The statement is true even if we A is an invertible affine transformation.*

Proof. Let $\mathcal{S} = \{S \subseteq [n]\}$. Let A act on $\mathcal{S}$ by mapping S to $A(S)$ such that $\chi_{A(S)}(x) = \chi_S(Ax)$. It is not hard to see that this action is bijective. For a function $g : \mathbb{F}_2 \to \mathbb{R}$,

$$(g \circ A)(x) = \sum_{S \subseteq [n]} \hat{g}(S)\chi_S(Ax) = \sum_{S \subseteq [n]} \hat{g}(S)\chi_{A(S)}(x) = \sum_{S \subseteq [n]} \hat{g}(A^{-1}(S))\chi_S(x)$$

Thus, $\widehat{g \circ A}(S) = \hat{g}(A^{-1}(S))$.
It is also easy to see that $\widehat{g \times \chi_U}(S) = \hat{g}(S \oplus U)$, where $S \oplus U$ is the symmetric difference of S and U.
Let $\phi : \mathcal{S} \to \mathcal{S}$ be defined as $\phi(S) = A^{-1}(S) \oplus U$. It follows from the above discussion that $\hat{h}(S) = \hat{f}(\phi(S))$, and that ϕ is bijective. This implies that the multiset $\{|\hat{h}(T)|\}_{T \subseteq [n]} = \{|\hat{f}(\phi(T))|\}_{T \subseteq [n]}$ is the same as the multiset $\{|\hat{f}(S)|\}_{S \subseteq [n]}$.
A similar proof works when A is an invertible affine transformation.

2.2 Bent functions

Definition 2. *A bent function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is a function with the property that $\forall S \subseteq [n]$, $|\hat{f}(S)| = \frac{1}{2^{\frac{n}{2}}}$*

Note that bent functions are only defined when n is even. Henceforth, we shall denote the set of bent functions on n variables by $\mathcal{B}_n$. The following is a useful characterization of $\mathcal{B}_n$ due to Rothaus[14]:

Lemma 2. *Let f be a boolean function. Then $f \in \mathcal{B}_n$ if and only if every non-zero derivative $\Delta_u(f)$ of f is balanced i.e. $\forall u \in \mathbb{F}_2^n \setminus \{0\}$, $\mathbb{E}_x \Delta_u(f) = \mathbb{E}_x(-1)^{f(x)+f(x+u)} = 0$.*

2.3 Quadratic boolean functions

Any boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ can be represented as a polynomial in $\mathbb{F}_2[x_1, x_2, \ldots x_n]$. The degree of the least degree polynomial that represents f is called the algebraic degree of f.
A function is called *quadratic* if its algebraic degree is at most 2. We shall denote the set of quadratic functions by $\mathcal{D}_n^2$. We will be interested in quadratic functions of a special form:

Definition 3. *For an even integer k, a quadratic function $p \in \mathbb{F}_2[x_1, x_2, \ldots x_n]$ is said to be in k-IP (Inner Product) form if*

1. *p is homogenous and $deg(p) = 2$.*
2. *If $x_{i_1}x_{i_2}$ and $x_{j_1}x_{j_2}$, where $i_1 \neq i_2$ and $j_1 \neq j_2$, are monomials occuring in p, then $\{i_1, i_2\} \cap \{j_1, j_2\} = \emptyset$, or in other words, the monomials are disjoint.*
3. *Except for some k variables, every variable occurs in exactly one monomial.*

Whenever a function is in 0-IP form, we shall simply say it is in IP form.

Definition 4. *The inner product function on n variables is $IP_n(x) = x_1x_2 + \ldots x_3x_4 + \ldots x_{n-1}x_n$.*

We shall now state a powerful lemma that describes the structure of quadratic functions over $\mathbb{F}_2$ (Theorem 6.21, 6.30 in [10]). The lemma has been reinterpreted in terms of the definition introduced above.

Lemma 3. *Let n be even, and let p be a quadratic function in $\mathbb{F}_2[x_1, \ldots x_n]$. Then there exists an $A \in GL_n(\mathbb{F}_2)$ and an even integer $k \in [n]$ such that $(p \circ A)(x) = q(x) + l(x)$, where $q(x)$ is in k-IP form, and $l(x)$ is a linear polynomial in $\mathbb{F}_2[x_1, \ldots x_n]$.*

The following is an obvious corollary:

Corollary 1. *Let n be even, and let p be a quadratic function in $\mathbb{F}_2[x_1, \ldots x_n]$. Then there exists an invertible affine transformation T, an even integer k, and a constant $c \in \mathbb{F}_2$, such that $(p \circ T)(x) = q(x) + c$, where q is in k-IP form.*

2.4 Parity decision trees

Parity decision trees are an extension of ordinary decision trees where one may query the parity of a subset of variables. In particular, the queries are the form "is $\sum_{i \in S} x_i \equiv 1 (mod\ 2)$?", where $S \subseteq [n]$.
In a similar manner, one can define randomized parity decision trees as a probability distribution over all deterministic parity decision trees such that for every input, the expected error of the algorithm is bounded by a constant $\epsilon < \frac{1}{2}$.
Let R^f be a randomized decision tree for f with error bound ϵ, and let $C(R^f, x)$ be the highest number of queries made by R^f on x. Then the randomized decision tree complexity of a function f, denoted by $R^{\epsilon}_{\oplus}$, is $min_{R^f} max_x C(R^f, x)$.

3 Testing quadratic bent functions

The goal of this section is to prove Theorem 1. For the remainder of the section, we shall denote the set of quadratic bent functions by $\mathcal{B}_n \cap \mathcal{D}^2_n$.
Let $A \subsetneq \mathcal{D}^2_n$ be a property of quadratic functions. The following is straight forward to verify:

Fact 1 *Let $f \in \mathcal{D}^2_n \setminus A$. Then $dist(f, A) \geq \frac{1}{4}$. In other words, for any function $g \in \mathcal{D}^2_n$, $g \notin A \Leftrightarrow g$ is $\frac{1}{4}$-far from A.*

This is basically a corollary of the fact that the distance between two quadratic polynomials over $\mathbb{F}_2$ is at least $\frac{1}{4}$. We now define the notion of testing under degree two promise.

Definition 5. *Let $A \subseteq \mathcal{D}^2_n$ be a property. The problem of testing A under degree two promise is the following:*
Given oracle access to $f \in \mathcal{D}^2_n$, determine with high probability ($\geq \frac{2}{3}$) whether

- *$f \in A$, or*
- *$f \notin A$.*

We denote the query complexity of testing A under degree two promise by $Q^*(A)$.

Let $Q(A)$ denote the query complexity of $\frac{1}{4}$-testing $A \subseteq \mathcal{D}^2_n$. A simple observation relates $Q^*(A)$ and $Q(A)$:

Lemma 4. *For any $A \subseteq \mathcal{D}^2_n$, $Q(A) \geq Q^*(A)$.*

Proof. Let T be a $\frac{1}{4}$-tester for A. Then, by Fact 1, T also tests A under degree 2 promise.

Our aim shall be to lower bound $Q^*(\mathcal{B}_n \cap \mathcal{D}^2_n)$, and we shall use ideas from [5] to do so. But first we will look at an alternate formulation of the Rothuas criterion.

3.1 Rothaus criterion revisited

There is a natural way to interpret a homogenous quadratic polynomial in $\mathbb{F}_2[x_1, \ldots, x_n]$ as a graph on n vertices.

Definition 6. *Let $p \in \mathbb{F}_2[x_1, \ldots x_n]$ be a degree 2 homogenous polynomial. Then the graph G_p associated to p is the following:*

1. $V(G_p) = [n]$
2. $\forall i \neq j$, $\{i, j\} \in E(G_p)$ *iff the monomial $x_i x_j$ is present in p.*

In a similar manner, one can associate a homogenous quadratic polynomial p_G to every simple graph G.
We now define the notion of 2-$\oplus$-coloring of graphs which will be useful in stating an alternate formulation of the Rothaus criterion (Lemma 2).

Definition 7. *Let G be a simple graph, and $c : V(G) \to \{0, 1\}$ be an assignment of colors to the vertices. Then c is called a 2-$\oplus$-coloring of G if:*

1. $\exists v \in V(G)$, $c(v) = 1$
2. *For every vertex v, the number of 1-colored neighbours of v is even.*

The following is an equivalent way of looking at the Rothaus criterion for homogenous quadratic polynomials:

Lemma 5. *Let p be a homogenous quadratic polynomial in $\mathbb{F}_2[x_1, \ldots x_n]$. Then p is bent iff G_p is not 2-$\oplus$-colorable.*

Proof. ($\Rightarrow$) Suppose p is bent. For sake of contradiction, let us assume that G_p has a 2-$\oplus$-coloring $c \in \{0, 1\}^n$. Let us fix some variable x_i that occurs in p. Note that p can be written as $p(x_1, \ldots, x_n) = x_i(\sum_{j \in N(i)} x_j) + p'$, where $N(i)$ denotes the neighbours of i in G_p, and p' is a quadratic polynomial which does not depend on x_i. Also, $\Delta_c(p) = \Delta_c(x_i(\sum_{j \in N(i)} x_j)) + \Delta_c(p')$.
We know that

$$\Delta_c(x_i(\sum_{j \in N(i)} x_j)) = x_i(\sum_{j \in N(i)} x_j) + (x_i + c_i)(\sum_{j \in N(i)} (x_j + c_j)).$$
$$= x_i(\sum_{j \in N(i)} c_j) + c_i(\sum_{j \in N(i)} x_j)$$

Notice that the coefficient of x_i in the above expression i.e. $\sum_{j \in N(i)} c_j$, is the parity of the number of 1-colored neighbours of i, and since c is a 2-$\oplus$-coloring, it must be zero. Thus, the derivative $\Delta_c(p)$ does not depend on x_i.
Since our choice of i was arbitrary, the above argument would imply that $\Delta_c(p)$ does not depend on any of the n variables, making it a constant. By Lemma 2, this is a contradiction since c is a non-zero direction and p was assumed to be bent.
($\Leftarrow$) This direction can be proved using a similar argument: if the derivative of p in some non-zero direction u is unbalanced, u can be interpreted as a 2-$\oplus$-coloring of G_p.

It turns out that the 2-$\oplus$-colorability of a graph G can be related to the invertability of its adjacency matrix.

Lemma 6. *A simple graph G is 2-$\oplus$-colorable iff its adjacency matrix $A(G)$ is singular.*

Proof. Assume that the vertex set is given by $[n]$. The color assignment is a vector $c \in \{0,1\}^n$. For every vertex i, introduce the equation $\sum_{j \in N(i)} c_i = 0$, where $N(i)$ denotes the neighbourhood of i. This equation essentially says that the number of 1-colored neighbours of vertex i is even. The graph is 2-$\oplus$-colorable iff the above system of equations has a non-zero solution which happens iff $A(G)$ is singular.

Combining Lemma 5 and 8, we get the following corollary:

Corollary 2. *A homogenous quadratic polynomial p is bent iff $A(G_p)$ is non-singular.*

3.2 Parity decision trees and communication complexity

We shall be interested in studying the randomized parity decision tree complexity of determining whether a given adjacency matrix of a simple graph is invertible. We begin by looking at the following communication complexity problem:

Definition 8. *Alice and Bob have matrices A and B in $M_n(\mathbb{F}_2)$ respectively, and they want to know if $A+B$ is non-singular over $\mathbb{F}_2$. We denote this problem by Det_n.*

Let $RCC_\epsilon(Det_n)$ denote the randomized communication complexity of Det_n when the protocol is allowed public randomness, and $RCC^p_\epsilon(Det_n)$ the complexity when only private randomness is allowed. (See [9] for the definition randomized communciation complexity). The following result lower bounds the randomized communication complexity of Det_n [16].

Lemma 7. $RCC^p_\epsilon(Det_n) = \Omega(n^2)$

A result of Newman [12] shows that for any function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$, $RCC^p_{\epsilon+\delta}(f) \leq RCC_\epsilon(f) + O(\log n - \log \delta)$. Since we are dealing with the case of bounded error probability i.e. ϵ, δ are small constants, we conclude:

Corollary 3. $RCC_\epsilon(Det_n) = \Omega(n^2)$

We now introduce a problem related to Det_n:

Definition 9. *The problem $AdjDet_n$ is the same as Det_n except that the matrices that Alice and Bob have i.e. A and B, are adjacency matrices of simple graphs..*

It's not hard to see that in the communication complexity paradigm, $AdjDet_n$ and Det_n have the same complexity.

Lemma 8. $RCC_\epsilon(AdjDet_n) = O(RCC_\epsilon(Det_n))$

Proof. Clearly, $RCC_\epsilon(Det_n) \geq RCC_\epsilon(AdjDet_n)$. We will prove the inequality in the other direction.
Let A be an arbitrary matrix in $M_n(\mathbb{F}_2)$. Consider the $2n \times 2n$ matrix A' given by $\begin{pmatrix} 0 & A^t \\ A & 0 \end{pmatrix}$. A' is a symmetric matrix by construction and it can be easily verified that $det(A) \neq 0 \Leftrightarrow det(A') \neq 0$.
Let P be a protocol for $AdjDet_n$. We will use P to design a protocol for Det_n. Suppose Alice and Bob have matrices A and B respectively. Alice and Bob construct A' and B' from A and B as defined above. Notice that $(A+B)' = A' + B'$. Thus, to determine if $A + B$ is nonsingular, they simulate the protocol P on A' and B'.

We now relate the communication complexity of $AdjDet_n$ to its parity decision tree complexity via a lemma stated in [5]:

Lemma 9. *Let $f : \{0,1\}^n \to \{0,1\}$, and let $R^\epsilon_\oplus(f)$ denote the randomized parity decision tree complexity of computing f with error ϵ. Then, the randomized (public coins) communication complexity of computing $f(a \oplus b)$ with error ϵ when Alice has a and Bob has b, where $a, b \in \{0,1\}^n$, is at most twice of $R^\epsilon_\oplus(f)$.*

Proof. It is easy to see that the parity queries made by the decision tree can be simulated by two bits of communcation between Alice and Bob. This shows that $RCC_\epsilon(f(a \oplus b)) \leq 2 \times R^\epsilon_\oplus(f)$.

Corollary 4. $R^{\frac{1}{3}}_\oplus(AdjDet_n) = \Omega(n^2)$

Proof. $R^{\frac{1}{3}}_\oplus(AdjDet_n)$ denotes the randomized parity decision tree complexity of determing if a given adjacency matrix is nonsingular with error at most $\frac{1}{3}$. The result follows from combining Lemma 9 with Lemma 8 and Corollary 3.

3.3 Proof of Theorem 1

We now come back to the task of lower bounding $Q^*(\mathcal{B}_n \cap \mathcal{D}^2_n)$.

Lemma 10. $Q^*(\mathcal{B}_n \cap \mathcal{D}^2_n) \geq R^{\frac{1}{3}}_\oplus(AdjDet_n)$

Proof. Let us suppose we have a tester T that tests $\mathcal{B}_n \cap \mathcal{D}^2_n$ under degree two promise. We build a randomized parity decision tree $\mathcal{T}$ that computes $AdjDet_n$ by simulating the queries made by T.
Suppose the input to the decision tree is the $n \times n$ adjacency matrix A. Recall from the previous section that the graph associated to A can be interpreted as a homogenous quadratic polynomial $p_A \in \mathbb{F}_2[x_1, x_2, \ldots x_n]$.
Let $c = (c_1, c_2 \ldots c_n) \in \mathbb{F}^n_2$, then for a graph G on the vertex set $[n]$, by $G[c]$ we mean the induced graph on the vertex set $\{i \in [n] | c_i = 1\}$ i.e. the induced graph on vertices which have been assigned 1.

Notice that quering p_A at $(c_1, c_2, \ldots c_n)$ is the same as the parity of the number of edges in $G_A[c]$, where G_A is the graph obtained by viewing A as an adjacency matrix.
$\mathcal{T}$, on input A, simulates the behaviour of T on p_A in the following way:

1. Whenever T tosses a coin, $\mathcal{T}$ does the same.
2. Whenever T queries p_A at $(c_1, c_2, \ldots c_n)$, T is essentially computing the parity of the number of edges in $G_A[c]$, which can be simulated by $\mathcal{T}$ in a single parity query to the matrix A.
3. $\mathcal{T}$ accepts A if T accepts p_A, otherwise $\mathcal{T}$ rejects.

Clearly, the query complexity of $\mathcal{T}$ is the same as that of T. Notice that $\mathcal{T}$ accepts A iff T accepts p_A, and by assumption, T accepts p_A iff p_A is bent. By Corollary 2, p_A is bent iff A is nonsingular. Thus, $\mathcal{T}$ accepts A iff A is nonsingular.

Theorem 1 now follows by combining Lemma 4 and 10 and Corollary 3:

$$Q(\mathcal{B}_n \cap \mathcal{D}_n^2) \geq Q^*(\mathcal{B}_n \cap \mathcal{D}_n^2) \geq R_{\oplus}^{\frac{1}{3}}(AdjDet_n) = \Omega(n^2)$$

4 Testing bent functions

The goal of this section is to "lift" the lower bound for testing $\mathcal{B}_n \cap \mathcal{D}_n^2$ to a lower bound for testing $\mathcal{B}_n$. We begin by analyzing the Fourier spectrum of quadratic Boolean functions.

4.1 The Fourier norm of quadratic functions

Lemma 11. *A quadratic polynomial $p \in \mathbb{F}_2[x_1, \ldots x_n]$ in IP form is bent. (See 3)*

Proof. Notice that if p is in IP form, then the corresponding graph G_p must be a perfect matching . Thus, it suffices to show that a perfect matching does not have a 2-$\oplus$-coloring (Corollary 2).
In a perfect matching, every vertex is the sole neighbour of some vertex, and if colored 1, would violate a condition for 2-$\oplus$-coloring. Thus, no vertex can be colored 1, and hence no 2-$\oplus$-coloring is possible.

The next two lemmas are useful in determing the Fourier transform of an arbitrary quadratic function.

Lemma 12. *Let $p \in \mathbb{F}_2[x_1, \ldots x_n]$ be in k-IP form. Then there are exactly 2^{n-k} non-zero Fourier coefficients of p each having absolute value $\frac{1}{2^{\frac{n-k}{2}}}$.*

Proof. Let us assume without loss of generality that the first $n-k$ variables are present in p. One can think of p to be in IP form as a polynomial in $\mathbb{F}_2[x_1, \ldots x_{n-k}]$. Then, by Lemma 11, p is a bent function in $\mathbb{F}_2[x_1, \ldots x_{n-k}]$, and $\forall S \subseteq [n-k]$, $|\hat{p}(S)| = \frac{1}{2^{\frac{n-k}{2}}}$.

Thus, as a polynomial in $\mathbb{F}_2[x_1, \ldots x_n]$, we have $\forall S \subseteq [n-k]$, $|\hat{p}(S)| = \frac{1}{2^{\frac{n-k}{2}}}$, and $\forall S \subseteq [n],\ S \cap [n-k+1, n] \neq \emptyset$, $|\hat{p}(S)| = 0$.

Lemma 13. *Let p be a quadratic polynomial in $\mathbb{F}_2[x_1, \ldots x_n]$. There is an even integer $k \in [n]$ such that p has exactly 2^{n-k} non-zero Fourier coefficients each having absolute value $\frac{1}{2^{\frac{n-k}{2}}}$.*

Proof. By Lemma 3, there is an $A \in GL_n(\mathbb{F}_2)$ such that $(p \circ A)(x) = q(x) + l(x)$, where $q(x)$ is in k-IP form, and $l(x)$ is a linear function. Note that adding a linear function to a Boolean function $f(x)$ is the same as multiplying $(-1)^{f(x)}$ with a character function.
Hence, by Lemma 1, we have $\{|\hat{p}(S)|\}_{S \subseteq [n]} = \{|\widehat{(p \circ A + l)}(S)|\}_{S \subseteq [n]}$ as multisets.
Also, $\{|\widehat{(p \circ A + l)}(S)|\}_{S \subseteq [n]}$ is the same as $\{|\hat{q}(S)|\}_{S \subseteq [n]}$. Since q is in k-IP form, Lemma 12 completes the proof.

4.2 Proof of Theorem 2

We now prove a lemma which will play a pivotal role in proving Theorem 2.

Lemma 14. *Let $f \in \mathcal{B}_n \setminus \mathcal{D}_n^2$ and $g \in \mathcal{D}_n^2 \setminus \mathcal{B}_n$. Then, $dist(f, g) \geq \frac{1}{4}$.*

Proof. Let $f \in \mathcal{B}_n \setminus \mathcal{D}_n^2$ and $g \in \mathcal{D}_n^2 \setminus \mathcal{B}_n$ be arbitrary. We want to show that $dist(f, g) \geq \frac{1}{4}$. We now compute $\langle (-1)^{f(x)}, (-1)^{g(x)} \rangle$:

$$
\begin{aligned}
&|\mathbb{E}_x (-1)^{f(x)} (-1)^{g(x)}| = |\sum_{S \subseteq [n]} \hat{f}(S)\hat{g}(S)| \\
&\leq \sum_{S \subseteq [n]} |\hat{f}(S)||\hat{g}(S)| \\
&= \frac{1}{2^{\frac{n}{2}}} \sum_{S \subseteq [n]} |\hat{g}(S)| \text{ (Since } f \text{ is bent)}
\end{aligned}
$$

By Lemma 13, we know that, for some even $k \in [n]$, exactly 2^{n-k} Fourier coefficients of g are non-zero and have value $\frac{1}{2^{\frac{n-k}{2}}}$. Thus,

$$\sum_{S \subseteq [n]} |\hat{g}(S)| = 2^{\frac{n-k}{2}}$$

But $k > 0$, otherwise $g \in \mathcal{B}_n \cap \mathcal{D}_n^2$, which contradicts our assumption. Also, the quantity $2^{\frac{n-k}{2}}$ is maximum at $k = 2$. Thus, $\langle (-1)^{f(x)}, (-1)^{g(x)} \rangle \leq \frac{1}{2}$.
Note that $|1 - 2 \times dist(f, g)| = |\langle (-1)^{f(x)}, (-1)^{g(x)} \rangle|$. This immediately gives $\frac{1}{4} \leq dist(f, g) \leq \frac{3}{4}$, which completes the proof.

We state a result due to Chen et al.[6] in a form that is suitable for application in our setting:

Lemma 15. *Let $\mathcal{P}_1$ and $\mathcal{P}_2$ be two properties of Boolean functions that have testers (possibly two-sided) T_1 and T_2 respectively. Let the query complexity of tester T_i be $q_i(\epsilon, n)$. Suppose $dist(\mathcal{P}_1 \backslash \mathcal{P}_2, \mathcal{P}_2 \backslash \mathcal{P}_1) \geq \epsilon_0$ for some absolute constant ϵ_0. Then, $\mathcal{P}_1 \cap \mathcal{P}_2$ is testable with query complexity $max\{q_1(\epsilon, n), q_1(\frac{\epsilon_0}{2}, n)\} + max\{q_2(\epsilon, n), q_2(\frac{\epsilon_0}{2}, n)\}$*

In its original form, the lemma has been proven for the case when T_1, T_2 are one-sided, and q_1, q_2 are independant of n, but the lemma can be easily seen to be valid in the more general case.
We are now in a position to prove our main theorem:

Proof (Proof of Theorem 2). It is well known via [1] that $\mathcal{D}_n^2$ is ϵ-testable with constant number of queries (say $q_1(\epsilon)$) . Suppose there is a tester that ϵ-tests $\mathcal{B}_n$ using $q_2(\epsilon, n)$ queries. By Lemma 15, we have that there is a tester that makes $max\{q_1(\epsilon, n), q_1(\frac{\epsilon_0}{2}, n)\} + max\{q_2(\epsilon, n), q_2(\frac{\epsilon_0}{2}, n)\}$ queries to ϵ-test $\mathcal{B}_n \cap \mathcal{D}_n^2$. Lemma 14 determines ϵ_0 to be $\frac{1}{4}$ and we set $\epsilon = \frac{1}{4}$. Thus, we have a tester that makes $max\{q_1(\frac{1}{4}, n), q_1(\frac{1}{8}, n)\} + max\{q_2(\frac{1}{4}, n), q_2(\frac{1}{8}, n)\} = q_1(\frac{1}{8}, n) + q_2(\frac{1}{8}, n)$ queries to $\frac{1}{4}$-test $\mathcal{B}_n \cap \mathcal{D}_n^2$. By Theorem 1, and the fact that $q_1(\frac{1}{8}, n)$ is a constant, we get $q_2(\frac{1}{8}, n) = \Omega(n^2)$, which completes the proof.

5 Testing $\mathcal{B}_n \cap \mathcal{D}_n^2$ via folklore

Most of the content of this section is folklore and we mention it here for the sake of completeness. Our goal is to show that testing $\mathcal{B}_n \cap \mathcal{D}_n^2$ reduces to testing if a given function is isomorphic to the inner product function $IP_n(x)$ under the action of invertible affine transformations.

Definition 10. *The problem of testing g-isomorphism under the action of a group H (on the space $\mathbb{F}_2^n$) is to distinguish with high probability between the following two cases:*

- *$f \in Orb_H(g)$*
- *f is ϵ-far from every function in $Orb_H(g)$.*

given oracle acccess to f, and ϵ as an input parameter. By $Orb_H(g)$ we mean the orbit of g under the action of H i.e. $Orb_H(g) = \{g(h(x)) | h \in H\}$.

We now state a folklore lemma without proof.

Lemma 16. *The problem of testing g-isomorphism under the action of a group H has query complexity $\log_2(|H|)$.*

Lemma 17. *Let f be a Boolean function. Then $f \in \mathcal{B}_n \cap \mathcal{D}_n^2$ iff there is an invertible affine transformation A and a constant $c \in \mathbb{F}_2$ such that $(f \circ A)(x) = IP_n(x) + c$.*

Proof. Notice that the statement is trivially true if $deg(f) > 2$. Thus, it suffices to show that a quadratic function f is bent iff it is affine-isomorphic to $IP_n(x)$ upto an additive constant.

Let f be a quadratic function . By Corollary 1, there is an invertible affine transformation A, an even integer k, and a constant $c \in \mathbb{F}_2$, such that $(f \circ A)(x) = q(x) + c$, where q is in k-IP form. Lemma 12 and 1 together imply that f has exactly 2^{n-k} non-zero Fourier coefficients each having absolute value $\frac{1}{2^{\frac{n-k}{2}}}$.
Now f is bent iff k is zero, and k is zero iff q is in IP form. The fact that any quadratic function in IP form is equal to the inner product function $IP_n(x)$ upto a permutation of the variables completes the proof.

Corollary 5. *The problem of testing $\mathcal{B}_n \cap \mathcal{D}_n^2$ reduces to IP-isomorphism testing under the action of invertible affine transformations.*

Proof. Let H be the group of invertible affine transformations, and let T be a tester for testing affine-isomorphism to $IP_n(x)$ with query complexity $q(\epsilon, n)$ and error parameter δ. We show that T can be used for testing $\mathcal{B}_n \cap \mathcal{D}_n^2$ with $O(q(\epsilon, n))$ query complexity.
Suppose the input function is f. The tester T' for $\mathcal{B}_n \cap \mathcal{D}_n^2$ first runs T on f, and then on $f + 1$. If either of the tests returns a positive answer, T' accepts f, otherwise it rejects f.
In the case $f \in \mathcal{B}_n \cap \mathcal{D}_n^2$, by Lemma 17, either $f \in Orb_H(IP)$ or $f + 1 \in Orb_H(IP)$, and T' accepts f with error at most 2δ.
Notice that, by an argument similar to the proof of Lemma 17, $\forall g \in Orb_H(IP)$ and $\forall c \in \mathbb{F}_2$, $g + c \in \mathcal{B}_n \cap \mathcal{D}_n^2$. Hence, if f is ϵ-far from $\mathcal{B}_n \cap \mathcal{D}_n^2$, then both f and $f + 1$ are ϵ-far from $Orb_H(IP)$, and T' rejects f with error at most 2δ.
Finally, the query complexity of T' is twice as that of T.

For the case when H is the group of invertible affine transformations, $|H| = O(2^{n^2})$, and by Corollary 5 and Lemma 16, the query complexity of testing $\mathcal{B}_n \cap \mathcal{D}_n^2$ is $O(n^2)$, which is tight due to Theorem 1.

6 Conclusions and open problems

We have shown that testing $\mathcal{B}_n$ requires $\Omega(n^2)$ queries. To the best of our knowledge, no nontrivial upper bounds are known for this problem. We conjecture an exponential lower bound for testing $\mathcal{B}_n$.
Unfortunately, since we "lift" the lower bound for $\mathcal{B}_n \cap \mathcal{D}_n^2$ to a lower bound for $\mathcal{B}_n$, and the lower bound for $\mathcal{B}_n \cap \mathcal{D}_n^2$ is tight, our current proof cannot yield anything better than $\Omega(n^2)$. In fact, it seems unlikely that our proof technique i.e. connection to parity decision tree complexity, would do any better.
On the other hand, we feel that our proof technique might yield lower bounds for other properties of quadratic functions, and this might be an interesting direction to explore.

Acknowledgements

The author would like to thank Sourav Chakraborty, Nitesh Jha, Satya Lokam, Partha Mukhopadhyay, and Prajakta Nimbhorkar for useful discussions and pointers to relevant literature.

References

1. Alon, N., Kaufman, T., Krivelevich, M., Litsyn, S., Ron, D.: Testing low-degree polynomials over gf(2). In: RANDOM-APPROX 2003. pp. 188–199
2. Blais, E.: Testing properties of boolean functions (2012), (PhD Thesis)
3. Blum, M., Luby, M., Rubinfeld, R.: Self-testing/correcting with applications to numerical problems. In: STOC. pp. 73–83 (1990)
4. Chakraborty, S., Fischer, E., García-Soriano, D., Matsliah, A.: Junto-symmetric functions, hypergraph isomorphism and crunching. In: IEEE Conference on Computational Complexity. pp. 148–158 (2012)
5. Chakraborty, S., Kulkarni, R.: Testing properties of linear functions via parity decision trees (2013), (Unpublished)
6. Chen, V., Sudan, M., Xie, N.: Property testing via set-theoretic operations. In: ICS. pp. 211–222 (2011)
7. Fischer, E.: The art of uninformed decisions: A primer to property testing. Science 75, 97–126 (2001)
8. Kaufman, T., Sudan, M.: Algebraic property testing: the role of invariance. In: STOC. pp. 403–412 (2008)
9. Lee, T., Shraibman, A.: Lower bounds in communication complexity. Foundations and Trends in Theoretical Computer Science 3(4), 263–398 (2009)
10. Lidl, R., Niederreiter, H.: Finite fields / Rudolf Lidl, Harald Niederreiter ; foreword by P.M. Cohn. Cambridge University Press Cambridge ; New York, 2nd ed. edn. (1997), http://www.loc.gov/catdir/toc/cam029/96031467.html
11. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes (North-Holland Mathematical Library). North Holland Publishing Co. (Jun 1988), http://www.worldcat.org/isbn/0444851933
12. Newman, I.: Private vs. common random bits in communication complexity. Inf. Process. Lett. 39(2), 67–71 (Jul 1991), http://dx.doi.org/10.1016/0020-0190(91)90157-D
13. O'Donnell, R.: Analysis of boolean functions (2012), http://www.analysisofbooleanfunctions.org
14. Rothaus, O.: On bent functions. Journal of Combinatorial Theory, Series A 20(3), 300 – 305 (1976), http://www.sciencedirect.com/science/article/pii/0097316576900248
15. Rubinfeld, R., Shapira, A.: Sublinear time algorithms. Electronic Colloquium on Computational Complexity (ECCC) 11(013) (2011)
16. Sun, X., Wang, C.: Randomized communication complexity for linear algebra problems over finite fields. In: STACS. pp. 477–488 (2012)

ECCC ISSN 1433-8092

http://eccc.hpi-web.de